Influence of the Privacy Issue in the Deployment and Design of Networking Robots in European Urban Areas

Alberto Sanfeliu[1], Maria Rosa Llácer[2],Maria Dolors Gramunt[2], Albert Punsola[3], Yuji Yoshimura[3]
[1]*Institut de Robòtica i Informàtica Industrial (UPC-CSIC){sanfeliu@iri.upc.edu},*
[2]*Grup de Recerca en Dret Privat, Consum i Noves Tecnologies (GREDINT-UB-SGR){marilo.gramunt@ub.edu; mrllacer@ub.edu}*
[3]*Barcelona Urban Ecology Agency {AlbertPunsola@bcnecologia.net}*

Abstract - In this article we analyze how the privacy issue will affect in the deployment and design of Networking Robots in European urban areas. Privacy means the way to guarantee self control on private data that can be processed by the Networked Robots. We start analyzing the technical capabilities of networked robots in public and private spaces, the legal framework and technical solutions. Then we present the main European Directives and how they affect in the Networked Robots. Next we go in the legal criteria for privacy compliance analyzing the surveillance utilities and the wireless communication systems. We also discuss the current legal framework for ubiquitous computing and analyze the anonymous processing for mobility management purposes using the Bluetooth scanning sensor. Finally we present some open questions

Keywords: Privacy, legal issues, network robot systems, autonomous robots

1. Introduction

At the present days, the term Ethics has become an important topic that has been extended to all the fields including robotics [24]. Ethics as defined in *Encyclopædia Britannica* "*also called moral philosophy* (is) the discipline concerned with what is morally good and bad, right and wrong. The term is also applied to any system or theory of moral values or principles" In the context of computers, "computer ethics" is defined in Sanford Encyclopedia of Philosophy as the field "that studies ethical problems aggravated, transformed or created by computer technology".

However, when we talk about Ethics in complex socio-technical systems, for example robotics, it is probably better looking in the legal theory, rather the moral theory (Asaro [1]). In [2], Asaro analyses how legal theory might be applied to robots. Schweitzer in the article "Robotics - chances and challenges of a key science" [14], discusses the challenges in the development of robots into intelligent machines and describes some examples in several fields, e.g, service and education. Solum in [29], argues if an artificial intelligent (a robot) become a legal person, and McNally and Inayatullah [15] discuss about the rights of robots

The fact that robots move in public and private space would multiply the number of opportunities in which law, surely, will be involved. This is because some of the tasks that the robots would be able to perform include interaction with citizens and the variability of the environment and it will lead necessarily to different situations which cannot be completely foreseen. The service and companion robots will act in a very different way that the industrial robots do at present. Networking robots in the street will be autonomous and will change behavior according to changing circumstances, although they will rely on a basic pattern related to the work assigned to them. But, even so, the number of unexpected events in the street will grow high compared to a factory. More uncertainty will lead to more conflict scenarios.

Robots in the public sphere have to face legal challenges according to what they are and according to what they could potentially do. This is not just because they are robots, but because they are new unclassified moving objects and the legislators have very little empiric knowledge of them. Consequently, as the capabilities and behaviors of the robots are better known and understood, it would become much easier to face properly legal challenges. It has to be underlined that it would be a mistake to consider legal challenges in relationship with the development of networking robotics as mere "obstacles to be removed". The right approach consists in considering how to introduce robots in the public sphere without interfering in the fundamental legal principles that European nations have given to themselves.

Of the different legal issues related to robot activities, see [26], we will discuss in this article the *Privacy* issue. The term *Privacy* refers to the way of guarantying self control in private data when personal information circulation mixes with technical data. In order to deploy robots and make extensive the deployment of Network Robot Systems (NRS) [27], it is required to know the norms foreseeing for the treatment and use of the citizens' personal data, because these norms represent the limits to the activities that the robots will be able to do. But, certainly the study of the *Privacy* issue will help to engineers and robot manufacturers to develop secure robots, which will be accepted by people.

The deployment of cameras everywhere and specifically in the cities has increased the interest to improve the *Privacy* issue in our legislation. However this was not the most important issue, the registration of digital data and its extensive use in databases made the *Privacy* issue an important topic in our present laws. When we think in deploying robots in cities allowing them circulating in the streets and performing different tasks to improve the quality of life in urban areas, then this issue become even more important. The reason is that the Network Robot Systems can potentially use personal data mixed with technical data, trough their cameras, sensors or any other type of capturing device or processing technique.

Examples of the *Privacy* issue can be found everywhere. For example, if a robot captures the image of traffic light or a bench nothing happens, but if the camera captures people's face then it becomes personal data that should be treated by country laws. This example –that could be extended to other sensors- shows that networking robot deployment in cities involves not only technical or social challenges, but also legal ones.

Fig1. The Privacy issue: how to assure privacy compliant robots

1.1. Technical capabilities of networked robots in public and private spaces: the relationship with personal data

In the field of Ubiquitous Networking we can notice that we are in the context of M2M (Machine to machine) relations, where devices, used or transported by a person, are able to detect each other. The identification of a person done by a device can be linked with the person own profile in a database. The *Internet of things* makes easy the capability to localize a person (owner or user), to know his or her profile, mix and cross personally identifiable information and keep a decision towards him or her. Robots can be equipped with several devices, for example: Radio Frequency Identifications (RFID), Bluetooth, WLAN, sensors, or cameras. Networked robots are autonomous, and they are able to change behaviors according to circumstances and to create information by themselves: for instance, they can store and create new profiles to identify and qualify somebody according to them. We may point out too that the personal information is mixed with the technical data. That's why self control on private data leads to a technical debate too: the legal framework implies technical solutions.

Networking robots deployment in urban areas, involves the processing of different kind of personal data:

- *Image, voice or biometrical data*: they can be used for obtaining personal data if they identify a person without disproportionate efforts. But also, if we process a personal situation, we could also obtain a profile of a person and make further decisions on the concrete person. We could even remark that in some situations, we do not need to identify the person to take a decision. For instance, if a robot detects a suspicious or an abnormal movement done by a person, the system can refuse to provide him a service (for example, let him enter in a building). Even if we

obtain the profile with anonymous data, we can assess that there is a personal identification, because a concrete decision is taken according to a predetermined profile.

- *Traffic or locating data, produced by connections between sensors, readers and databases*. A networked system is able to detect the persons (for instance, if they carry a tag or by their biometrical data), to network the information, to take an individual decision, or to create and accumulate knowledge about them. It is important to clarify that using the network, the robots can not only identify a person, but they can also know where the person is (for example, by a GPS), or at what time it has been in a specific location and so on. In these cases, the network uses several types of processes: identification, transmission and processing.

- *Content data*. It is also personal data. They refer to personal information stored in a database and processed to obtain new information about an individual. Medical history, police information, consumer profile are examples of information referred to somebody. A networked system is able to communicate and cross all types of information. When robots transmit information to a database any type of processing remains possible.

It is important to differentiate between public and private goals of processing. Legal framework differs if robots are used for public or private services.

In public services, we can make the difference between public utilities and surveillance. Public utilities involve activities as street cleaning, rubbish collection or the estimation of the number of pedestrians in a fixed area. As a matter of fact, this kind of processing can perfectly work without the need of personal data, by simply making the data anonymous. Instead, the surveillance issue deserves a special regulation: surveillance is certainly essential for public security, but involves a risk for private freedom too. Robots equipped with cameras or sensors can be used to identify people according to a profile or to send this information to different databases with surveillance purposes (we will go into details on section 6).

In requested or private services, data processing is similar to any service provided by any private electronic communication operator. Robots can provide information services, or can even accept payments for the service: for instance a pedestrian asks for information about the recommended routes, restaurants or stores in the neighborhood (we will go into details on section 7.1).

In relationship with RFID implementations, Weinberg stands out three main privacy threats: the geographic surveillance, profiling and action [33]. It is unquestionable that everyone carrying a tag can be identified or shown his data by any tag reader controller. But as a matter of fact, the problem is more serious because data processing allows profiling: tags keep and accumulate personal information and their contents can be transmitted to databases and can be crossed or associated with additional data. The profile of an individual can be easily used to take a concrete decision, based on new knowledge about somebody who does not have the means to know or to react against an automatic action.

It is obvious that privacy law foresees all these topics. Sometimes, there is no legal constraint because networked activities do not involve personal data: for instance, if a robot detects an object (without connection with an individual) there is neither personal information to protect nor identification function. But frequently the presence of personal data becomes an important element to be foreseen. In the next part we will deal with the European meaning of privacy and, mainly, with the repercussions in robots' design and manufacturing. In the field of public surveillance, we will see that national laws develop special framework for video surveillance (quite "traditional" way of surveillance), but that networked devices remain in the field of general framework because there are not yet specific provisions.

1.2. Privacy legal framework and technical solutions: privacy friendly robots

In relationship with privacy, the legal aspect is not connected with errors or robot malfunction, but just with the capabilities that are included in a correct performance of a task. A good example is the networked robot navigation which depends on cameras that capture people's images. This issue poses a privacy problem, a delicate subject in European Law, which is extensively regulated. The same could be said in the case of other personal data like secret codes or personal figures that can be captured by sensors.

In Europe, the privacy legal framework is addressed to enhance the power of citizens on their own information. But this main goal involves more participants, as manufacturers, software designers and Public Administration. In the field of robots, the software and hardware industry should know the area of *secure activity* from the privacy point of view. Privacy friendly robots become a guarantee for everybody.

The privacy legal framework foresees:

- *Data Processors' duties*: for instance, devices, communications and databases must fulfill different security levels and guarantee confidentiality. For this reason, industry must guarantee these technical issues before their commercial distribution. For instance, encryption of tags or electronic communications becomes an important issue.

- *Citizens' rights*: citizens must be able to know the presence of devices on public or private spaces. If a law does not allow data processing, they may conserve the capability to decide about it. We emphasize on technical meanings to allow previous information and to make possible the consent on data processing: for instance, RFID devices should contain blockers, in order to allow de-activating the tag if there exist the legal possibility to oppose to data processing.

It is necessary that the devices may have the technical capability to allow the legal compliance: the devices may allow self-determination that is the possibility to say no and control what kinds of data are disclosed. They may offer the technical capability to make data anonymous; and offer people to choose de-activation. This means information and visibility on tags or readers. The devices must allow compliance with data processing principles too: they must be prepared to use accurate data, adequate, relevant and not excessive for the application. Particularly, they must respect the criteria of protecting sensible data (information revealing racial or ethnic origin, opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life). Moreover, they can also be able making possible the control by judge or public authorities.

Finally, we must point out that the scheme "data processor' duties / citizens' rights" falls when law foresees exceptions. Exceptions allow the data processing and weaken personal control capabilities if there is a public interest to be protected, considered in a democratic society.

1.3. The European framework: a high legal degree approach

The European framework deserves a far-reaching protection. In European areas, data processing is controlled by law: a correct processing is a lawful one. This premise is important for the citizenship acceptance, avoid claims and sanctions and ensure robot manufacturers and dealers.

There is an important Acquis on data protection law which lays directly on fundamental rights (1). The proprietary approach, well-known in the United States, has no relevant importance among European authors [25] [21]. According to the European approach, privacy addresses directly to freedom. There is not a capability to use personal information subjected to exceptions based on personal rights: the whole system is based on the protection of self determination, as an aspect of a fundamental right. The defense

of the private sphere, originally argued by Warren and Brandeis [32], must be at the moment completed in a positive sense: privacy points to the capability to control our profile by unwished uses and this include invasive environments. So, privacy means self control on private data and self-determination. We take the term "control" in the sense of self-determination, settled by the decision from the German Federal Constitutional Court (1983), on the German Census Act (Volkszählungsurteil) [3]). The decision lies on the concepts of human dignity and self-development and settles the famous "right to informational self-determination", understood as the capability of the individual to decide himself when and within what limits information about his private life should be communicated to others.

Privacy, in its functional sense, relates to the concept of *dignity*. Privacy means self-determination, which is the fundamental right to control several aspects of individuals' life, especially in the field of personal information. This is a core issue in Europe, developed by different authors [21] and by Courts' decisions (for instance, the Spanish High Constitutional Court Decision 292/2000, 30.11.2000). Instead, in the United States the "control" issue only refers to a theory used to conceptualize privacy. The conceptualize privacy is necessary when the protection of private life is constructed in the frame of the tort law. However, the control theory, has been surpassed by other theories involving all kind of data, not only data in the private sphere, but also behaviors in public spaces. In this sense, privacy becomes contextual [30]. Our article focuses on the European approach, where law defines the data concept and draws citizens' rights. Nowadays, this right-based approach has an important challenge: its harmonic connection with manufacturers' and software architects' work. Some European Authorities' documents (10) (11) (12) and (13) detect this question, highlight the challenge to translate law principles into technical devices and relate the privacy issue with the security issue.

Data processing is an activity which makes knowledge and places power in data controllers' hands. Controllers obtain great amounts of private data by different means: traffic and navigation data (where do I link, at what hour and so on), locating data (where I am and where I go), identification data (images of my face or my body or my voice) and content data (which are my preferences, what kind of services do I ask for, what is the service cost). Indeed, the knowledge of personal information gives others the capability to decide about our lives: for instance, who knows about us can use our profile to refuse automatically to supply a service: this can be a way of discrimination. The processing and use of all these data places citizens in a weak situation. Usually citizens ignore the presence of the devices and that these devices can obtain data that citizens are not aware, because they have been programmed by someone that decides the aims of the devise without taken into account the privacy issue.

The main European Directives are:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (3). This is the main legal reference. As all directives, this one has been adopted by national legislations. In this way data protection has become a common objective in the UE countries and special government bodies have been created to watch on this objective and enforce the law if necessary. The Directive states that data processing shall be done under precise principles (transparency, legitimate purpose and proportionality) and foresees National Supervisors.

- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications (5). This Directive contains the criteria for making data processing legitimate in connection with the provision of publicly available electronic communications services in public communications networks in the Community (art. 3.1). Non-public communication services remain under Directive 95/ 46/EC. However Directive 2002/58/CE has been amended by Directive 2009/136/CE (7). The new text applies better to new applications based on the devices for data collection and identification, which could be contactless devices, for example using radio frequency. It improves the security of processing and, in the case of a personal data breach, stands the duty for the provider of publicly available electronic communications services, to notify the personal data breach to the competent national authority (art. 4).

- Directive 2006/24/EC (6) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. This Directive aims to harmonize Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (art. 1).

Regulations on video surveillance are developed by national frameworks. National laws translate the general Directive principles but, there are differences related with the national organization of public security. The restrictive focus on personal data processing in Europe has its roots in the historic misuse of this type of data for criminal purposes by undemocratic regimes before and after World War II. In recent years the balance between security on one hand and freedom on the other has been altered by international terrorism in favor of security, but Europe retains strongly its principles of protecting individual rights.

2. Networking robots deployment in European urban areas: legal criteria for privacy compliance

2.1. Robots without privacy concerning devices

It is obvious that robots are able to fulfill a large number of functions where personal information is not always required. For instance, robots used for street cleaning and rubbish collection do not need personal data; neither it is required for robots that help handicap people if they do not keep identification data.

When a robot works without recording or processing personal data or any private information which allow identifying a person, the manufacturer or user remain free of legal privacy constraints. An information is personal if an individual can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (art. 1 Directive 95/46/EC). If a robot is placed to count persons on a square, to evaluate the frequency of visitors in a museum or to make statistics on the number of vehicles circulating on a road, no personal data are needed. When data are anonymous, personal data and technical options can be used without submission to legal constraints.

Nowadays, if the robot is able to read tags or the registration number of a vehicle, a data processing is done. Law stands a principle of proportionality, so robots shall be able to adapt their technical capabilities to functions they are designed for. If personal data are not essential for a robot task, it is better not to record or process it, in order to avoid future problems to the manufacturers and users.

We can still analyze another topic, quite frequent in ubiquitous computing. Apparently the analysis of behavioral patterns taken from concrete anonymous movements does not hurt legal framework just because data are anonymous. But when robots act an individual just because he matches a profile, there are some use of data (for instance, his movements are interpreted as suspicious). In spite of the "*personal* data" concept (cfr Directive 95/46/EC), these anonymous figures are registered and processed to select individuals. The processing aims to create an instrument to detect personal information without focusing on the concrete characteristics of the individual, in order to make an automated decision. In this sense, this procedure only could be possible if necessary in order to protect the vital interests of the individual's data or for the performance of a task carried out in the public interest or in the exercise of official authority (art. 7 criteria). For instance, an alarm sounds when a device detects a vital danger for the subject.

2.2. Robots equipped with privacy concerning devices: the role of users and manufacturers

If a robot reads a tag, a smart card or biometrical data, they can identify a person directly or by identifiers carried by individuals. We have already underlined the capability to track individuals or to cross information and to create individual profiles. These data can be transmitted from tag to a database, even remote. Tags, readers, databases and wireless communications must fulfill the privacy framework.

It is true that manufacturers are not concerned by the use of the devices developed by them. The data controller is responsible of a legal compliant processing (the manager who puts a robot in a building or on the street and decides the data processing goal). Apparently, manufacturers are only designing a product and its use does not affect them. Not really: this article addresses both to manufacturers and the end users. And manufacturers are in charge of integrating privacy rules into the design and construction of information systems and devices [16].

The data controllers have the duty to fulfill a legal processing: they must give information (the presence of tags or readers), they must obtain the consent of people for a personal data processing or verify that there is a legal exception, they must ensure the capability to oppose to the processing and to exercise the other individual rights (tag blockers). And obviously they must ensure the legal level of security according to national law (higher when the processing involves sensible data).

But the role of producers is essential: they must ensure the capability of devices to fulfill the law and they are also certainly influence on privacy standards. Some authors have highlighted the rule-making power of technology and networks [22]. Architectural designs and technological capabilities create default rules, so the circulation of information and general practices work in a predetermined way and lead users to an opt-out behavior. For instance, open standards force to adopt privacy-enhancing technologies, as cryptography, to preserve confidentiality in the transmission of messages. By making easy the European privacy standard, producers do not only adopt a good market strategy; also, they ensure a social approval and the capacity, for data processors, to fulfill legal duties.

In this way, EU has adopted the Directive 2009/140/EC (8) that has modified the Directive 2002/21/CE (4) by introducing a new Chapter (Chapter IIIa) entitled *Security and integrity of networks and services.* The scope of this Chapter is to prevent and minimize the impact of security incidents on users and interconnected networks. In this way, Member States shall ensure that the companies providing public communications networks or electronic communications services take appropriate technical and organizational measures to manage the risks posed by the security of networks and services. The Directive adds that these measures shall ensure a level of security appropriate to the risk presented.

Privacy by design is an essential way for exercising the self-determination protected by law. So law and technology should work together: law states the guarantees for autonomy in the disclosure or not of personal information; privacy-enhancing technologies (PET) are the tool to make it possible. As Cohen states, legal protection alone cannot create or guarantee informational privacy [5]. In this sense, official and independent technical approvals become important to promote privacy-enhancing technologies [31] and ensure non burdensome procedures for customers or citizens to exercise their rights [12].

The Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (10) insists on the use of PET to promote privacy, fundamental rights (so public interest) and consumers' confidence. The European Commission supports the use of PET and proposes several actions:

- supporting the development of PETs and identifying the need and technological requirements of PETs

- supporting the use of available PETs by data controllers (this implies promoting the use of PETs by industry, ensuring the respect for appropriate standards in the protection of personal data through PETs, for instance by standardization)
- encouraging consumers to use PETs to raise awareness and facilitate consumers' informed choice (Privacy Seals)

Technical standards involve both producers and governors. Producers can promote policy rules (*lex electronica* as conduct codes issued from governance) and governments generally support this tool foreseeing some mandatory standards. Some authors in Europe insist on official approvals for privacy friendly devices, on the convenience of the precaution principle (this is the option for sensible ICT implants [10], useful in the future to connect persons and robots) and the equipment with technical standard allowing an immediate opt-in or opt-out [21] (16).

3. Surveillance utilities

In this article we focus only on some examples where sensors, common in networked robots, are used. However, we don't try to be exhaustive. Examples allow to state privacy problems and to suggest solutions which could be extended to other situations.

3.1. Robots equipped with cameras or recorders in public and private areas

Deployment of networking robots in urban areas implies the processing of different kinds of data (image or voice data, traffic or locating data, content data) which can be used for two very different goals: public services (including surveillance) and requested or private services. The surveillance use is regulated by national provisions applying to video surveillance, but we must highlight some recent attempts to adapt these traditional issues to current technical situations, for example the cyber surveillance.

Data processing in surveillance has several characteristics: citizens become massively identifiable because the street is not always an anonymous space and an automated processing remains possible (devices can register, recognize, act and they are able to create autonomous knowledge). However, surveillance is also convenient in a democratic society and our analysis shall pay attention to the processing allowed under legal exceptions. Art. 13.1 of the Directive 95/46/EC (3) recognizes that the Member States may restrict some obligations and rights when it is necessary to public security or to prevention, investigation, detection and prosecution of criminal offences. And more precisely, art. 15 of the Directive 2002/58/EC (5) submits restrictions on privacy protection in public communication services as stated in the following functional and coherent argument: they shall constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security. All these premises lead us to some evidence: in the surveillance context, the information duty can remain essential, but sometimes the processing will be lawful without consent, restricting the capability to have some control on it. Nevertheless, the European States have a strong role in guaranteeing fundamental rights and this goal inspires the legal control on exceptions.

The idea is also presented in art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1): its first paragraph contains the right to respect the private and family life, home and correspondence. The second one adds: "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

But exceptions can only run under the control of the law, in the context of a State whose role is instrumental, submitted to (and legitimated by) constitutional law and fundamental rights. This means that militarization of security is not an unavoidable fact and that technology is an instrument submitted to law. Legislators must assess the risk to scarify privacy in the name of security ([11], p. 37). Technology resident in robots will be legal depending on this assessment (for example Directive 2006/24/EC on the retention of data can be a good example). But must they go forward? Must everybody be registered, monitored, profiled? The limits are on European Convention for the Protection of Human Rights and on the regulator's awareness on his function and the value of civil liberties. We go in some concrete details of the characteristics of this surveillance process.

Surveillance includes two processing modalities: surveillance in public areas and surveillance in private areas. In Europe it is accepted that citizens have the control in expectations on personal data in public areas.

Data processing in surveillance in public or semi public areas is reserved to State security forces. They are the database controllers and, so, they are responsible of them if they cause injuries or make an infraction. Surveillance in private areas is relevant under privacy law when data processing exceeds household activities. In this context, owners (single owners or condominium) are controllers of databases and surveillance requires the initiative of a private processor. For instance a camera is placed on a building's entrance.

The purpose of surveillance can justify data processing with a lower level of guarantees. But the whole situation must fulfill the legal criteria that support the exceptional treatment of the fundamental right of privacy and when the law does not support a processing data, it must be anonymous. For instance, as face o body are personal data, an official approval is required to install surveillance cameras in a public area. A picture of someone is undoubtedly personal data, because the definition of this concept includes information about a person that could lead to identification of that person (definition of personal data in article 2 of the Directive 95/46CE (3)).

Member States have developed national provisions to channel the resource of private data to surveillance goals. The Opinion 4/2004 of Article 29 Data Protection Working Party (9) shows a list of national provisions on video surveillance. To install cameras for surveillance purposes some special law is needed to sustain some exceptions, especially to avoid citizens' consent (for instance French Law n° 95-73 (17) -art. 10.1 and 19- related with general Law n° 78-17 (16)). Some countries have developed other resources, as conduct codes or special provisions from National Authorities. For instance, in United Kingdom, the Information Commissioner (http://www.ico.gov.uk/) published a CCTV data protection code of practice in 2000, used to help ensure that the use of CCTV complies with the Data Protection Act 1998 (24). In Italy, the *Provvedimento generale sulla videosorveglianza* (20) concretes the application of general principles and recognizes the limitation of consent.

The regulation of cameras handled by urban robots strongly depends on national regulations. Certainly, the principles are similar, through the Directive 95/46/CE (3), but the details (system, authorizations) will not be uniform. For instance the Belgian Law (14) and (15) regulates the complete possibilities of installation of cameras: in open public places, in closed places open to the public and, finally in closed places not opened to the public. In all these cases, an official visa is needed. Instead, the Spanish law divides the consideration of cameras into two legal frameworks: the installation for the purpose of surveillance in public (open or closed) spaces (Organic Law 4/1997 (22)), and the installation in private spaces, by a private company (Law 23/1992 (23)).

We can summarize that data processing for surveillance in public areas is reserved to police or State security forces. Data must be adequate, relevant, not excessive, not further processed in a way incompatible with the purposes of the special law, and must be kept for a limited period. The purpose of cameras must be specific and lawful and the recourse to video surveillance must be proportional and

adequate (cfr art. 2 of the Provvedimento generale sulla videosorveglianza (20)). The Public Administration's authorization verifies the requirements needed by a robot with a camera in order to safeguard the rights of citizens. This statement is valid for static cameras (prior authorization and obligation to inform on their existence), but should be rectified indeed for mobile cameras depending on the State (implicit information if they support static cameras; and installed even without previous authorization if there exists an urgency). But law limits the access and cancelation rights and certainly weakens, in this point, the capability of citizens' control.

The deployment of robot cameras in urban areas for surveillance purposes have to take into account the following legal premises:

- The competence to decide the installation of video surveillance engines is reserved to public security forces, and generally verified by official Commissions. Its use is included in activities to prevent crime and protect persons and their properties.
- The processing of images or voice is lawful when installation and lawfulness of cameras are allowed and checked by authority. The individual right of consent disappears because there is a legal permission.
- The rights to access or opposite can be denied to the benefit of general security.
- The databases storing images or sounds depend on public authorities. For instance, the local police must fulfill the procedure to create a database, to notify and register it and is responsible about security obligations.

Surveillance in private areas, when exceeds the personal or household activities, involves the processing of third persons' data. Law becomes, again, the guarantee of a correct processing and the instrument to avoid the individual consent of citizens. Data must fulfill the mentioned general standard (must be adequate, relevant, not excessive, not further processed in a way incompatible with the purposes of the special law, and kept for a limited period). In this point there are differences between national States: in some of them processing deserves a public authorization, in other countries, the operation remains under the further inspection by the Supervisory Authority.

The owners of private areas are responsible of databases (they are legal controllers because state the purposes and means of the processing). They become processors in a subordinated activity in relationship to public security, but generally the processing is outsourced to a professional company (a body who processes personal data on behalf of the controller, art. 2.e of Directive 95/46/CE (3)). We can see that networking robots in private areas will require the initiative of the private processor. The installation of cameras will be normally submitted to authorization, or as in Spain, reserved to companies of security, which competences are recognized by law, through a legal recruitment (under legal conditions) and submitted to the inspection of the Supervisory Authority. Obviously, the authorization of a judge to follow criminal investigations is not the question in this moment.

3.2. What about cyber surveillance?

If networking is to be used for surveillance purposes, a very high level law shall foresee this situation. In our society, with a permanent feeling of insecurity and where technical resources can be unlimited, this becomes a social question too.

New devices allowing the automated acquisition of body movement or facial traits can detect strange or suspicious conducts or identify a person by a specific part of his face or body. They can connect these data with elements of personal identity, as passwords. This is an automated processing, very fast, because it doesn't involve any human activity. The control on citizens, by these procedures, can become a restriction on human freedoms and should only be justified if they are necessary in a democratic society and proportionate to the achievement of specific purposes.

Quite recently, the German Constitutional Court published a decision ruling about the constitutionality of secret online searches of computers by government agencies (on 27 February 2008). This landmark constitutes a new basic right, stemmed from the personality rights in German Constitution (the right to informational self-determination was introduced in 1983) "to the confidentiality and integrity of information-technological systems". The decision stops a law of the federal state of North-Rhine Westphalia which aimed to allow the government agencies to "covertly observe and otherwise reconnoiter the Internet, especially the covert participation in its communication devices and the search for these, as well as the clandestine access to information-technological systems among others by technical means"[1]. The Constitutional Court stands that individuals depend on these kinds of systems to express their personality: so restrictions in this field directly affect their freedom and capability to express their personality. The Court considers that systems must fulfill the proportionality principle and prevent indiscriminate processing by government agencies without an approval by a judge in case of "factual indications for a concrete danger" for the life, body and freedom of persons or for the foundations of the state.

It is clear that the communication networks, even if they are handled by public services providers, are also protected by law in the sense that personal information remains "personal" and under legal principles. So, judicial control works on private spheres, but also on public or quite public ones. In this sense, in Europe, protection against government surveillance beyond our house is more solid than in an American perspective when some authors argue that an erosion of the Fourth Amendment could be possible in the field of ubiquitous RFID [28].

So the topic remains an open question, but we may consider that invisibility and permanency are a very strong characteristic of ubiquitous processing and this must be taken into account for its legal, ethic and sustainable development.

4. Wireless communications systems

4.1. Application of current legal framework to ubiquitous computing

Actually, wireless and mobile sensors (RFID, Bluetooth, mobile phones, Pocket PC) make citizens massively identifiable everywhere. They are highly important in networked robots because they interact by these means. The automated processing is permanent and it is possible to complete a permanent tracking of the behaviors and locations of individuals. Ubiquitous computing includes microprocessors into everyday objects and they are prepared to detect and to be interconnected (even placed on a person - or in a person as implants-). So an automated and permanent learning and profiling is possible because devices can change the profiling criteria and adapt themselves. The power imbalance between individuals and data processors becomes higher and risky for self determination; that’s why many authors discuss the lawfulness of processing in this field [18].

We can notice that the Information Society is a society of services, where robots can be placed to provide some kind of utilities to citizens. Devices’ utilities related with personal identity and individuals could be inexhaustible. For instance, sensors can be used to employee identification or building access. A robot can detect a tag carried by an individual and provide some information about the services in the quarter or even recognize the client when he or she returns. If the system recognizes a tag or an identifier, information can be stored, retrieved, crossed and remains permanently accessible and for several uses, without relationship with the kind of service or utility requested by the citizen. If a person pays for the service, financial data can be added. If the engine has the capability to mix stored information with sensible data, as health or medical data, the situation still becomes more delicate. It is

[1] http://www.bverfg.de/pressemitteilungen/bvg08-022.html

not necessary to think at the patient's medical history implanted in a tag; devices with a unique ID used to control sportsmen physical activity could reveal his fitness, but also can allow tracking him[2]. Loyalty cards or tags leaved in a consumer good can also become identifiers.

Devices are useful, but they can contain personal data that can be transmitted. If no information is provided when citizens disclose data, if they do not know for what the data can be used for or if there are tools to avoid the transmission of this information, the above mentioned imbalance is obvious. There is a "Cloud computing" allowing users to access technology-enabled services without real capabilities to control the technology infrastructure that supports them [4].

The permanent networking of individual information is a real possibility, by the devices they carry on (consumer goods equipped with tags, phone cells, implants) or by themselves (physical or biometrical data). The constant capability to store, transmit and process information allows a profiling always bring up to date. Concrete decisions on an individual are taken also automatically: for instance, the system denies access because of the suspicious characteristics of person physical profile. The result at privacy level is clear: ubiquitous computing operates invisibly, without citizen knowledge or consent, and it can make new knowledge and take decisions using these new data.

Individuals are just handled as a thing: they become an element of the so called *Internet of things*. Their presence in ubiquitous computing does not differ from any object made from smart dust. But these things are persons and they can enter in the network through many doors, opened with the same identity key that allows to gather what Rodotà calls the "electronic body" [23]. The identity concept is being submitted to a change: sometimes a name is not as important as the capability to contact a person. Poullet talks about "third generation data" [21] (cfr. Directive 2002/58/EC (5), art. 14.3 and w. 46) embracing an ID number, and any data which allow to reach a person and impose an automated decision.

There is not a specific legal framework for this kind of devices. But that does not mean that the activity remains free for users and producers: general Directive 95/46/EC (3) states the principles to be fulfilled. If communications are transmitted by a public service network, the service provider is submitted to Directive 2002/58/EC (5) and to data retention Directive 2006/24/EC (6), because it may fulfill a legal processing on traffic and location data. This is an important mention: the Directive 2009/136/EC (7) amending Directive 2002/58/EC (5) includes (art, 3) 'public communication networks supporting data collection and identification devices'. So the development of applications entailing the collection of information, including personal data, using radio frequencies, such as RFID, will be subjected to the ePrivacy Directive when they are connected or make use of public communication networks or services.

The European Data Protection Supervisor finds this provision positive as it clarifies that a number of RFID applications that falls within the scope of the ePrivacy Directive, and allows removing some uncertainty on this point and definitively removing misunderstandings or misinterpretation of the law (nº 18 (11)). Nevertheless, the Directive only applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community. It does not apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public and private communications networks and publicly accessible private networks as suggested the European Data Protection Supervisor (nº 66 (13)). So for example, Internet access could be available to the public not through a public network, but rather through what may be considered a private one, i.e. a privately operated network that is not under the 2002/58/CE (5), which is only protected by the Directive 95/46/EC (3), not related to the electronic communications. This remains a problem because, as European Data Protection Supervisor says: "As a result, the fundamental rights of individuals guaranteed by the ePrivacy Directive are not protected in these instances and an uneven legal situation is created for users accessing the same Internet access services through public telecommunications means vis-à-vis

[2] For instance, see Nike + iPod**,** www.apple.com/ipod/nike/run.html

those who access them via private ones. This despite the fact that the risk to individuals' privacy and personal data in all of these cases exists to the same degree as it does when public networks are used to convey the service".

However, the principles issued from general Directives 95/46/EC (3), or the Directive 2002/58/EC (5) in the frame of public communications networks, can apply to many situations and devices. Laws generally do not fit to a very concrete device: they state a protection to any interest and set rights and duties related to the function of a device. This procedure ensures an adaptation to novelties; but it is difficult to predict a long life of the Laws in the current technical evolution (15).

That is why lawyers shall make a contextual effort and consider the nature of data, the reason for the processing and the goal to be reached [18, p. 154]. Traditional data processing principles need a reinterpretation exercise in the field of ubiquitous computing. What is important in this context is that customers must be informed when they buy a smart object, activate a tag or when they approach to some reader able to identify them and use their data for many different purposes. So the data controller can use data only for stated purposes. Except if there is a legal exception (for example, law states a data control or a customer asks for a service where the data are necessary), the data should not be disclosed without the individual's consent, and he must be informed about who is collecting data and why, in order to keep the possibility to opposite, verify or modify his interest. Accountability originates from the introduction of legal principles in devices and robots in a secure manner. Security is also a main duty for controllers: data stored in tags, flows, and databases must remain secure from hackers' attacks and potential abuses.

We are going to consider some examples where robots are involved in privacy issues. Unless a law allowing cyber surveillance, as discussed above, a robot could not read personal identifiers indiscriminately. Some conditions are needed to ensure a legal processing.

a) *Example 1: Robots are used to control the entrance in private areas and they are equipped with readers*. If they are the tool to control employees' activity in a company, law gives employers the capability to verify their compliance and they do not need an individual consent. But they really need to inform of tracking and the pertinent goal of the processing. Nevertheless, a subcutaneous implant should not be pertinent, because it is possible to identify people by less invasive means. Instead, the European Group on Ethics in Science and New Technologies considers that this kind of implants should be justified for Alzheimer patients [10].

b) *Example 2: When in a concrete area there are many readers, can citizens be confident about they anonymous presence?* Perhaps they consent a concrete use of the identifier, but not other kind of uses. Is the content of my loyalty card or my health card accessible to other data controllers? Security is essential: an adequate encryption give confidence and preserve from legal breaches. Uniform labels could also be useful to disclose the presence of readers (10) and to ensure the capability to pull a blocker. The *"kill switch" technology is also necessary if the user has the capability to opt-in or to opt-out a default option* [12, p. 148]. We can point out that a generic consent is not a legal one: we can consent to activate a tag to enter a building; but this does not automatically allow the controller to give personal information to third persons or use them to particular purposes (for instance commercial purposes)[6].

c) *Example 3: A robot, in a public or private space, provides a service requested by a customer (for example, information about spectacles or leisure offers)*. First of all, the identity of customer is not relevant if the information is served by the robot itself. But if the provider sends information to a mobile device or charges it into customer account, personal data may be processed only for this purpose related with the requested service. Data are used to provide or to charge the service, but can not be given to third persons (always unless specific consent).

d) Example 4: A robot *uses anonymous data to take individual and automated decisions*. If a robot only recognizes and classifies movements, and learns about this information, data remain anonymous. But the processing may remain legal as a whole and European principles remain incompatible with data mining for tracking, distance manipulation and automated decisions [10].

4.2. The case of Bluetooth scanning sensor for mobility management purposes: technical options for anonymous processing

One of the services that could be provided by networking robots is mobility management. Mobility is a fundamental factor for the economic growth of cities and social sustainability [7]. Successful traffic management can overcome apparent contradictions like achieving economic development and at the same time protecting the environment. In consequence, a variety of sensors and methodologies have been proposed in order to study vehicle's behaviors and understand their patterns. In most cases, the approaches rely on Electromagnetic loop, Ultra Sonic Sensor or Origin Destination Survey (OD Survey). In addition, different types of Video Cameras from the infrared camera to closed circuit television (CCTV) offer solutions to identify a moving object for traffic data collection.

The recent advances in wireless and mobile devices such as mobile phones, navigation systems, Pocket PC and PDA, open new possibilities for data collection which could not be imagined just a few years ago. These wireless devices can act as sensors and be tracked to collect precise trajectory in space-time.

These developments have enabled the ability to use of Bluetooth sensors (BT sensor) for vehicle and pedestrian localization. Bluetooth is the global standard protocol (IEEE 802.15.1) for exchanging information wirelessly between mobile devices, using 2.4 GHz short-range radio frequency bandwidth. Ericsson started to develop it in 1994 and released it in 1998. It was designed to reduce the communication cost between the fixed and portable devices with low power consumption. Nowadays, it allows devices to communicate without the physical line between devices from 10m to 100m range, even if there exist some obstacles between them. One of the characteristics of Bluetooth is the device-discovery ability which permits to collect information about nearby Bluetooth devices as Media Access Control address (MAC address), device name and device type.

Although a variety of other project have used Bluetooth detection, many of them exploited its proximity detection mechanism for measuring the social network relation of people indoors and outdoors [2,3,4]. For instance, the Cityware project[3] applied this technique in public space for detecting individuals [19]. The purpose of this application is to understand people's behaviour and social networks through the combination of several techniques: human observation and pervasive technologies. In another line of research, the Innovative Cities of Next Generation (ICING) project[4] proposed a traffic management system by identifying the trajectory of vehicle through Bluetooth signal [34]. In this case, the goal was neither to count the number of passing cars nor to perform a precise count. The objective was to get the trajectory data and to validate both the methodology and the data obtained.

Based on this first experiment the Barcelona based firm, Bitcarrier[5] has developed and refined the techniques to come up with a patented technology that detects around 70 different devices per second. The immediate communication of these data to a centralized server enable allows visualizing them in real time on their web page[6]. This solution is effective for tracking vehicle and pedestrian movements

[3] http://www.cityware.org.uk/
[4] http://www.fp6-project-icing.eu/
[5] http://www.bitcarrier.com/
[6] http://www.bitcarrier.net/map/, Password: mediatest

and also for analyzing the patterns and trends of the movements of people across the city.

There are many privacy issues concerning this technology. The MAC address is a unique code that belongs exclusively to a specific device (PC, mobile, PDA, Car Navigation System), although exceptionally some makers release few devices with the same code not following the standard procedure. Nevertheless, this code can be considered as personal data because a link between the code, the device and the owner of the device is not impossible. This code consists in the combination of 6 alphanumeric pairs (Hexadecimal). The first 3 pairs are allocated to the company through the Institute of Electrical and Electronics Engineers (IEEE) and the last 3 are distributed to each device by the service provider company.

This information is useful to differentiate an individual Bluetooth device but rather ineffective to identify a specific person. Indeed, in order to know the owner, it needs to combine several datasets from different sources protected by service providers. Therefore, it is very difficult to achieve it practically and identify the owner. However, one can argue that there would be a possibility of uncovering personal data. The code which is, in principle, anonymous could become personal data if someone is able to establish the adequate connections between the different sources and obtain a link to a personal identity. But there is a technical solution that can avoid this to happen. A solution applied in some Bluetooth projects [7]. Following we describe an effective way to address this problem.

Keeping data anonymous is a secure issue. By using an adaptation of SHA (Secure Hash Algorithm) to BT sensor, it permits to generate anonymous trajectory data even if there is a record of these data in an archive without invading privacy. This happens as follows: when the sensor gets a MAC address, SHA algorithm generates an internal identifier with it. The original MAC address is erased at when the identifier is assigned. In consequence, it is not possible to retrieve the link between the generated number with the original MAC address as the identifier becomes anonymous with no possibility to make a link to any personal data. The advantage of hash algorithms is to be able to generate always the same output from a specific input. It doesn't need to save any state data in the archive. This scheme permits to perform an anonymous logging and identify trajectories of people without invading their privacy.

Within this legal framework, more than 5,300,000 unique codes at 11 points in Barcelona have been obtained during 8 months for the purpose of traffic and pedestrian management. Currently, several projects for mobility analysis are proceeding through collaboration with the Mobility Department of the Barcelona City Council, Technical University of Catalonia (UPC) and Massachusetts Institute of Technology (MIT).

5. Open questions:

There are a number of open questions that must be solved, we include here some of them:

- The framework should include the privacy compliance in standardization patterns. This would be an essential way for a realistic performance.
- Is it enough to ensure that data remain anonymous to fulfill privacy framework? We should rethink on the fact that only a movement can activate a bad reaction by a robot. Perhaps there are not a personal data in a traditional sense, but there is an abnormal processing of information under legal principles.
- The capability to identify an individual is changing to the electronically ability to reach a user. What really matters to deserve legal protection is the real capability to be reached through our own or foreign devices.
- Since the processing can be invisible, is consent still enough to ensure legal compliance (when processing is not allowed by a special legal permission)? Lawyers and manufacturers should think about the capability to be really proactive in some complex contexts.

- Patterns lead to uniformity: perhaps we should remind that the essence of democratic societies is the respect of individuals: everybody should act as it is socially expected? Who designs patterns? Is reductionism a collateral consequence of security and efficiency?

6. Conclusions

We have presented the key legal challenges on privacy issue related with robots deployment in public and private areas. Some conclusions on the privacy issues are the following ones:

- It must be made clear what legal challenges have to be faced in a concrete way. It is necessary to specify what personal data will robots be able to obtain and what is the possibility of processing these data according to: a) technical devices (sensors, integrated mobile cameras, fixes cameras, readers, databases etc) and b) tasks to perform (for instance to collect garbage is different from surveillance).
- The use of robot networking with data recording and storage devices for private purposes, including requested e-services, requires users' consent as is established in the general legal framework. However this users' consent shall not be necessary under some usual exceptions (for example, when data are anonymous). Anyway, it has to be taken into account that in some cases "usual exceptions" can involve risks and automated decisions as it has been explained in this article.
- On the hand of surveillance, there is a special legal framework. Individual guarantees decrease in order to protect public interest. This legal framework exists for video surveillance (cameras and sound recording engines). A legal framework for sensors and ubiquitous computing does not exist yet. Nowadays the processing of personal data must be restrictive or anonymous. However, there is the exception of data retention foreseen by the Directive 2006/24/CE allowing the disclosure of traffic and locating data to public authorities, if required, to follow criminal investigations to a public service provider.
- Legal framework needs an adaptation effort to changes that technology could bring. New devices and processing techniques demand an efficient empowerment which probably will result from a complex solution combining law, technique and self regulation.
- We should be especially attentive to the eventual ethical–legal questions that can raise the use of robots in the execution of their tasks, mainly when they affect to areas intimately related to the free development of the citizens' personality in a democratic society.

Acknowledgements

This work has been partially supported by CICYT project DPI2007-61452 and IST-045062 of the European Community Union.

References

[1] P.M. Asaro, «What Should We Want From a Robot Ethic?», *International Review of Information Ethics*, Vol, 6 (12/2006). http://www.i-r-i-e.net/inhalt/006/006_Asaro.pdf.
[2] P.M. Asaro, «Robots and Responsibility from a Legal Perspective», http://www.peterasaro.org/writing/ASARO%20Legal%20Perspective.pdf.
[3] Bundesverfassungsgericht, 15th December 1983, *EuGRZ*, (1983).
[4] A. Cavoukian: «Privacy in the clouds», *IDIS DOI* 10.1007/s12394-008-0005-z, *Springer* (Published online 18.12.2008) (2008).
[5] J.E. Cohen: «Examined Lives: Informational Privacy and the Subject as Object», *52 Stan. L. Rev.* (1999-2000), p. 1428.

[6] C. Colin, Y. Poullet: «Observation society and marketing: case study», *La autodeterminación informativa en la sociedad de la información y de la vigilancia*, coord. M.R. Llácer (Ed.), La Ley-Wolters Kluwer, Madrid, (2011).
[7] Commission of the European Communities. *Green Paper Towards a new culture for urban mobility*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0551:FIN:EN:PDF, (2007).
[8] D. Darquennes, Y. Poullet*:* « RFID: quelques réflexions introductives à un débat de société », *Revue du Droit des Technologies de l'Information* – n° 26 (2006).
[9] N. Eagle, A. Pentland: «Reality mining: sensing complex social systems». *Pers Ubiquitous Comput.* 10 (4): 255-268.
[10] European Group on Ethics in Science and New Technologies to the European Commission: *Opinion on Ethical Aspects of ICT Implants in the Human Body* (16.03.2005) (ec.europa.eu/european_group.../activities_en.htm).
[11] B. Hayes: "Arming Big Brother. The EU's Security Research Programme", Transnational Institute, TNI Briefing series, Nº 2006/1. www.statewatch.org/analyses/bigbrother.pdf
[12] L. Hildner: «Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level» 41 *Harv., C.R.-C.L. L. Rev.*, 2006, p. 165.
[13] V. Kostakos: «The privacy implications of Bluetooth», arXiv:0804.3752.
[14] S. Lawrence B., «Legal Personhood for Artificial Intelligences». *North Carolina Law Review*, Vol. 70, p. 1231, 1992. Available at SSRN: http://ssrn.com/abstract=1108671.
[15] P. McNally and S. Inayatullah, «The Rights of Robots: Technology, Law and Culture in the 21st Century» *World Peace Through Law Center: Law and Technology* (Winter, 1987); in *Futures* (Vol 20, No. 2, 1988), 119-136; and, in *Whole Earth Review* (No. 59, Summer 1988), rewritten in Sohail Inayatullah and Paul Wildman, eds. Futures Studies, Brisbane, Prosperity Press, 1998) (CD-ROM).
[16] M. Nagenborg, R. Capurro, J. Weber, C. Pingel: «Ethical regulations on robotics in Europe», *AI & Soc*, 2008, 349-366.
[17] T. Nicolai, E. Yoneki, N. Behrens, H. Kenn: «Exploring social context with the Wireless Rope». In: *On the move to meaningful internet systems, 2006: OTM 2006 workshops*, part I, LNCS, vol. 4277. Springer, Heidelberg, pp 225-242.
[18] H. Nissenbaum: «Privacy as contextual integrity», *79 Wash. L. Rev.*, 2004, pp. 147-148.
[19] E. O'Neill, V. Kostakos, T. Kindberg, Fatah gen. A. Schieck, A. Penn, D. Stanton D. Fraser, T. Jones: «Instrumenting the city: developing methods for observing and understanding the digital cityscape». In: *Ubicomp 2006: 8th international conference on ubiquitous computing, LNCS*, vol. 4206. Springer, Heidelberg, pp 315-332 (2006).
[20] E. Paulos and E. Goodman: «The familiar stranger: anxiety, comfort, and play in public places». In proceedings *CHI* 2004, ACM, pp. 341-350.
[21] Y. Poullet, A. Rouvroy: « Ethique et droits de l'homme dans la société de l'information », *Rapport général introductif à la session préparatoire organisée conjointement par l'UNESCO et le Conseil de l'Europe dans le cadre du suivi des SMSI* (2008). http://www.crid.be/newsletter/UK/2008/Crid-Newsletter-July-August-September2008.htm
[22] J.R. Reidenberg: «Lex Informatica: The Formulation of Information Policy Rules Through Technology», *Tex. L. Rev*. 76, 553-593 (1997-1998).
[23] S. Rodotà: Discorso del presidente, Relazione 2004 (Garante per la Protezione dei dati personali), www.garanteprivacy.it.
[24] A. Rouvroy: «Privacy, Data Protection, and the Unprecedented Challenges of Ambient Inteligence», *Studies in Ethics, Law, and Technology*, Berkeley Electronic Press, 2008.
[25] A. Rouvroy, Y. Poullet: «Self-determination as the "key concept". Reinventing Data Protection», *International Conference co-organized by the University of Tilburg, the Information Technology & Law Research Centre, University of Namur, and the Vrij Universiteit Brussels, 12-13 October 2007*. Brussels. Oct. 2007.
[26] A. Sanfeliu, A. Punsola, Y. Yoshimura, MR Llácer, MD Gramunt: «Legal Challenges for networking robot deployment in European urban areas: the privacy issue, Workshop on Network

Robots Systems», *IEEE International Conference on Robotics and Automation (ICRA2009)* Kobe (Japan), May 12th, 2009.
[27] A. Sanfeliu, N. Hagita, A. Saffiotti: «Network Robot Systems», *Robotics and Autonomous Systems*, Vol 56, Nº. 10, pp. 793-797, October 2008.
[28] J.M. Schmidt: «RFID and privacy: living in perfect harmony», 34 *Rutgers Computer & Tech. L.J.*, 2007-2008, p. 260.
[29] G. Schweitzer: «Robotics-Chances and challenges of a key science», *17th International Congress of Mechanical Engineering* (COBEM 2003), São Paulo, Brasil, November 10-14, 2003. http://www.mcgs.ch/web-content/Robotics.pdf
[30] H.T. Tavani: «Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy», *Metaphilosophy*, vol. 38, nº 1, p. 16, 2007.
[31] L.M. Ulatowski: «Recent Developments in RFID Technology: Weighing Utility Against Potential Privacy Concerns», 3 *ISJLP, I/S A Journal of Law and Policy for the Information Society*, 2007-2008, p. 636.
[32] S.D. Warren, L.D. Brandeis: «The right to privacy», *Harvard Law Review*, 14, nº 5, 193-220 (1890).
[33] J. Weinberg: «Tracking RFID», 3 *ISJLP, I/S A Journal of Law and Policy for the Information Society*, 2007-2008, p. 811.
[34] Yoshimura, Y., González, E., Punsola, A., Andrés, D., Cárdenas, F.: «Tools for process modelling and decision-making», ICING Final publishable report (2008). http://www.fp6-project-icing.eu/

Appendix: LEGISLATION AND LEGAL DOCUMENTS

EUROPEAN RULES

(1) European Convention for protection of human rights and fundamental freedoms (Council of Europe, Rome, 04.01.1950).
(2) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, Strasbourg, 28.01.1981).
(3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
(4) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002, on a common regulatory framework for electronic communications networks and services (Framework Directive).
(5) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
(6) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
(7) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
(8) Directive 2009/140/EC of the European Parliament and of the Council, of 25 November 2009, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications

networks and services.

EUROPEAN UNION DOCUMENTS

(9) Opinion 4/2004 of Article 29 Data Protection Working Party, on the Processing of Personal Data by means of Video Surveillance (11750/02/EN WP 89).
(10) Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), Brussels, 2.5.2007 COM(2007) 228 final.
(11) Opinion of 10 April 2008 on the Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ C 181, 18.07.2008.
(12) Article 29 Data Protection Working Party: Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) 00350/09/EN WP 159.
(13) Second opinion of 9 January 2009 on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ C 128, 06.06.2009, p. 28.

BELGIUM

(14) Privacy act, of 08.12.1992 (Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel).
(15) Installation and use of surveillance cameras Act, issued 21.03.2007 (Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance).

FRANCE

(16) Computing and Freedoms Act, issued 06.01.1978 (Loi relative à l'informatique, aux fichiers et aux libertés).
(17) Orientation and programming Security Act, issued 21.01.1995 (Loi d'orientation et de programmation relative à la sécurité), modified by Act 2006-64 (23.01.2006).

GERMANY

(18) Federal Data Protection Act, issued 18.05.2001(Bundesdatenschutzgesetz).

ITALY

(19) Personal Data Protection Code, issued 30.06.2003 (Codice in materia di protezione dei dati personali).
(20) Video surveillance, General provision adopted by the Garante (n. 49/April 2004).

SPAIN

(21) Data Protection Act issued 13.12.1999 (Ley Orgánica de Protección de Datos personales).
(22) Videosurveillance by Security Forces in Public Spaces, issued 04.'8.1997 (Ley orgánica 4/1997, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos).
(23) Private Security Act issued 30.07.1992 (Ley de Seguridad Privada).

UNITED KINGDOM

(24) Data Protection Act, issued 1998.